Naval Security Enterprise Newsletter

4TH QUARTER FY16 AND 1ST QUARTER FY17

INSIDE THIS ISSUE:

DUSN (P) Security Director's Corner

FAREWELL TO Mr. Jeffery W. Bearor who has taken a different position with the USMC. Over the last 3 years Mr. Bearor has been an inspirational leader for the DON Security Directorate and accomplished a multitude of actions while serving as the second DUSN (P) Senior Director for Security (SDS). Mr. Bearor' s leadership will surely be missed.

I am Steve Ulate, Deputy Director, and I will be performing the duties of the SDS until another SDS is assigned. I look forward to working with all of your leaders on a variety of security issues affecting the DON now and the near term. Our focus is to continue implementation of the Insider Threat program, Continuous Evaluation, Controlled Unclassified Information (CUI), SPēD certifications and work to mitigate the Personnel Security Investigations backlogs. There are many other security areas that will also be a priority for the DON Security Enterprise -- these are just a few. Again, I look forward to working with everyone in the community.

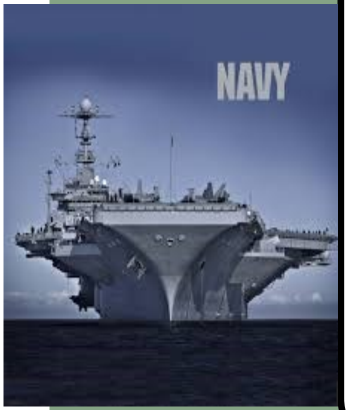
SharePoint Registration

The DUSN (P) Security Directorate would like to encourage readers to register for the CAC-enabled Security Directorate SharePoint website in order to receive the latest security announcements and updates posted on the website. To register for the SharePoint website click this website icon: Website

Community Updates

The DUSN (P) Security Directorate requests security professionals submit noteworthy stories or relevant articles to be featured in future editions of the newsletter. We are looking for articles that highlight individual achievement (s) and team successes within the DON. The Security Directorate would like to encourage more DON community involvement in order to facilitate better communication throughout the department. Members should feel free to send input(s) to the Security Education, Training, and Awareness Branch at: **DON_SECURITY_SETA_US@NAVY.MIL**

Information Security



FY 2016 Information Security Program Self Inspection and Program Management Classification Reports

The Department of the Navy (DON) is required to establish and maintain an ongoing self-inspection and oversight program to evaluate and assess the effectiveness and efficiency of our implementation of the information security program (ISP), per DoDM 5200.01-Volume 1. Deputy Under Secretary of the Navy (Policy) (DUSN (P)) Security Directorate (SD) collects data from commands throughout the DON utilizing the Self-Inspection Program (SIP) Data - due 31 August 2016, and the Agency Security Classification Management Program Data form (SF 311) - due 30 September 2016. The SIP data and the SF 311 are developed by and reported to the Information Security Oversight Office (ISOO) annually via DUSN (P) as the DON Senior Agency Official. The goal of the data collection is to evaluate the DON's protection of national security information and demonstrate its commitment to open Government through accurate and accountable application of classification and timely declassification actions.

Commands must use the current SIP data, pending the rewrite of the SECNAV M-5510.36. The self-inspection criteria in SECNAV M-5510.36, Exhibit 2C, no longer correlates with the reporting information required in the SIP data developed by ISOO. The DUSN (P) SD developed additional guidance, in order to assist commands with obtaining, maintaining, and providing a more detailed and accurate reporting of the required SIP data. Required action and documents were posted in TV 5 (DCN 2016UGENERAL-012510b) on 22 June 2016. ISOO revised the SF 311 in March of 2016, including a new section for the intelligence community (IC) who originally apply the originator controlled (ORCON) and originator controlled-U.S. Government (ORCON-USGOV) dissemination control markings. Required action and documents were posted in TV5 (DCN 2016UGENERAL-016112g) on 16 August 2016. Additional questions/concerns can be sent via email to DON_SECURITY_INFO@navy.mil.

Physical Security

Law Enforcement Officers Safety Act of 2004 (LEOSA)

After two years in writing and formal review, the Department of the Navy Law Enforcement Officers Safety Act (LEOSA) Program, SECNAV Instruction 5580.3, has been forwarded to the Secretary of the Navy for signature. The instruction should be reviewed by all current, retired and separated Department of the Navy law enforcement officers.

In accordance with DoD Directive 5525.12, LEOSA implements sections 926B and 926C of Title 18, United States Code (U.S.C.) and incorporates section 1089 of Public Law 112-239 for (military and civilian) law enforcement personnel within the DoD who possessed statutory powers of arrest or authority to apprehend pursuant to section 807(b) of Title 10, United States Code (also known as article 7 (b) of the Uniform Code of Military Justice).

Signed into law on July 22, 2004, LEOSA is intended to afford qualified active and retired law enforcement officers the privilege of carrying a concealed firearm in all 50 states, the District of Columbia, the Commonwealth of Puerto Rico, and all other U.S. possessions. By definition, qualified LEOSA is for those who were authorized by law to engage in or supervise the prevention, detection, investigation, or prosecution of, or the incarceration of any person for, any violation of law.

Requirements in meeting LEOSA standards, active law enforcement must attain service training qualifications for employment. Retired law enforcement must have served a minimum of 10 years of service. Those who completed training qualifications and probationary periods of employment, but were separated due to a service-connected disability are also eligible. For additional information email us at: DON_SECURITY_PHYS@NAVY.MIL

"If you See something Say something."

Personnel Security

Changes to Guidance Regarding Foreign Passport

Being a U.S. citizen and a citizen of another country is not prohibited or disqualifying for a security clearance eligibility, however there are qualifying conditions that must be met in order to obtain/retain a clearance. State Department guidance states that foreign passports are NOT to be destroyed, nor is it a requirement to relinquish a foreign passport to the security official. It is however, a requirement to disclose possession of a foreign passport to an appropriate security official for initial review and once annually as long as member retains a clearance. Ensure that the following statement is included on an foreign citizen's statement expressing their willingness to renounce foreign citizenship: "I understand travelling on a foreign passport or obtaining a new passport is reportable and will affect my eligibility and/or assignment to work in a sensitive position."

Secure Web Fingerprint Transmission Plus Enrollment (SWFT Plus Enrollment) The Department of the Navy (DON) transitioned to SWFT Plus Enrollment on 30 September 2016. The use of automated electronic fingerprint devices will greatly speed capture, submission, and processing time while providing higher quality images.

The Site Administrator will receive standard operating procedures for SWFT Plus and will be required to register and manage the local fingerprint operator user accounts for their subordinate, commands.

To establish a SWFT Plus user account, echelon I and II security mangers must register as a Site Administrator by completing and submitting Personnel Security System Access Request (PSSAR) Defense Manpower Data Center (DD Form 2962) which can be found at: https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT. Forward the completed form to our office: **DON_SECURITY_PERS@NAVY.MIL**

Industrial Security

NEW! **"Unsatisfactory Security Ratings" and "Facility Clearance Invalidations".** The Defense Security Service (DSS) has implemented a new notification procedure for "Unsatisfactory Security Ratings" and "Facility Clearance Invalidations issues for cleared contractors. DSS will officially notify the Deputy Under Secretary of the Navy (DUSN) (Policy) Security Office of using the tracker TV-5 system.

Once the DUSN (P) Security Office receives a notification, the Industrial Security Branch will select the appropriate security offices in TV-5 for official coordination, notification and official response on how the system command program office plans to proceed. The commands must decide to "continue or discontinue" performance on an affected contract (s).

Once the command responds, an official response is created and submitted to DUSN senior officials for review and signature. The information is then forwarded to DSS as a part of the official record. Some system command program offices have gone through the implemented procedures.

National Industrial Security Program Contracts Classification System (NCCS) DSS is continuing there NCCS enhancement testing with more and more Navy commands signing up to participate in testing phases. The current phase is a critical testing phase ICO the DD Form 254. This phase allows vendors to see their prime DD form 254s; require an agency name and address to be added to block 12 on the DD form 254. DUSN (Policy), Industrial Security Branch will provide updated NCCS information as received from DSS. For additional information please contact the Industrial Security Branch via email: **DON_SECURITY_IND@NAVY.MIL**

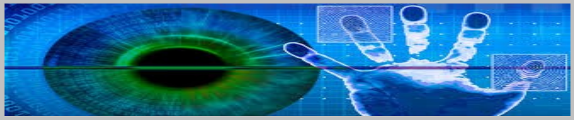
© Can Stock Photo - csp15045554

Enterprise Security

Identity Dominance System

How does the Department of the Navy support Identity Operations (IdOps)? One way in which the DON supports IdOps is through the development and fielding of the Identity Dominance System (IDS). IDS is the DON's biometrics Program of Record that provides the means to collect and process identity information in the conduct of maritime and expeditionary operations. There are three key aspects of this capability: 1) it enables forces to rapidly identify unknown individuals encountered in the conduct of operations; 2) it verifies unknown individual's claimed identity; and 3) enable forces to update, manage, and share identity information on friendly, neutral, and enemy individuals in support of Identity Operations (IdOps).

As we analyze the challenges within our ever-changing battlespace, we acknowledge a demand for enhanced IdOps due to the shift from traditional kinetic to cyber and asymmetric warfare. In collaboration with DoD and non-DoD IdOps stakeholders, the IDS program seeks to improve upon currently fielded technologies by leveraging investments in technology advancements and development efforts through research, evaluation, maturation and integration. By FY19, the goal of the IDS program is to implement a technology refresh (NextGen IDS) that incorporates a best-of-breeds solution to meet current and future DON requirements. NextGen IDS will provide the Operator with a lightweight, robust system that takes advantage of enhanced communication capabilities to achieve near real time database response. By designation from the IDS program office, PMS 408, the Naval Surface Warfare Center Dahlgren Division (NSWCDD) serves as the Technical Direction Agent leading the charge for NextGen IDS. The DUSN (Policy), Security Directorate, in collaboration with IDS personnel, ensures Navy IdOps has a voice within the DoD. For more information, questions/concerns on Identity Operations, please contact the Security Enterprise Branch at: **DON_SECURITY_ENTERPRISE@NAVY.MIL**



Acquisition Security

On 23 August 2016, a joint memorandum between the Office of the Under Secretary of Defense for Intelligence (OUSD (I)) and the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD (AT&L)) was signed, requiring a partnership between the two communities in order to provide support to the Defense Security Service (DSS) in addressing challenges identified when making risk-based decisions on behalf of the acquisition community. Some of these challenges include making National Interest Determinations for foreign-owned companies, as well as actions pertaining to facility clearances. OUSD (AT&L), OUSD (I) and DSS, with assistance from stakeholders, will jointly review the current DoD risk assessment and mitigation framework to synchronize these processes within the Department. In response to this memo, DSS is developing the Concept of Operations (CONOP) and is expected to be released by January 2017. DUSN (P) Security Directorate's current role in the execution of this memo is to coordinate with the Services and System Commands to ensure the appropriate individuals (i.e., Acquisition, Counterintelligence, Intelligence, Security) are gathered together to create an "integrated, multi-disciplinary framework to assess, and where possible, mitigate risk to classified U.S. technology and information resident in the cleared industrial base." A copy of the memo can be found on the DUSN (P) Security Directorate SharePoint Site. For additional information email us at: **DON_SECURITY_ACQ@navy.mil.**

Security Education, Training, and Certification

New Joint Personnel Adjudication System (JPAS) Training Courses

Effective 1 November 2016, the Center for the Development of Security Excellence (CDSE) retired the Joint Personnel Adjudication System (JPAS)/Joint Clearance and Access Verification System (JCAVS) Virtual Training for Security Professionals course PS123.16. As a result of the course retirement, students who are enrolled in the course will no longer be able to complete the course or take the exam. Alternate CDSE JPAS courses will be available after 10/31/16 and are listed below: JCAVS User Level 7 & 8: PS181.16; JCAVS User Level 10: PS182.16; and JCAVS User Levels 2 thru 6: PS183.16. Please visit Defense Manpower Data Center's (DMDC) JPAS website (click on Account Manager Policy) for information regarding DMDC JPAS account training requirements after 10/31/2016. For access to DMDC' JPAS website click here.

Naval Security Manager Course Update.

Beginning 1 December 2016, students requesting attendance to the Naval Security Manager Course (NSMC) are required to complete new prerequisite training before attending the course. The new prerequisites are online training courses through CDSE and include Introduction to Information, Personnel and Physical Security. In addition to the courses above, students will also have to complete the JCAVS User Levels 2-6 PS183.18, which will replace the JPAS/JCAVS Virtual Training for Security Professionals PS123.16. For more information and to view the FY17 schedule and course perquisites click here.

Points of Contact:

Mailing Address:

Deputy Under Secretary of the Navy,
(Policy) , Security Directorate
1000 Navy Pentagon, Rm 4E572
Washington, DC 20350

Email Addresses:

Acquisition Security
DON_SECURITY_ACQ@NAVY.MIL
Industrial Security
DON_SECURITY_IND@NAVY.MIL
Information Security
DON_SECURITY_INFO@NAVY.MIL
Enterprise Security
DON_SECURITY_ENTERPRISE@NAVY.MIL
Personnel Security
DON_SECURITY_PERS@NAVY.MIL
Physical Security
DON_SECURITY_PHYS@NAVY.MIL
Security Education, Training and Awareness
DON_SECURITY_SETA_US@NAVY.MIL

Newsletter Editor:
Tracy L. Kindle

Useful Links:

Department of The Navy, Security Executive:

http://www.secnav.navy.mil/dusnp/Security/Pages/Default.aspx

National Counterintelligence and Security Center:

https://www.ncsc.gov/index.html

Information Security Oversight Office:

http://www.archives.gov/isoo/

Security Professional Education Development:

http://www.cdse.edu/certification/index.html

Security Training Education and Professionalization Portal (STEPP)

http://www.cdse.edu/stepp/index.html

AMERICA'S NAVY
A GLOBAL FORCE FOR GOOD.™